

“Restricted” by such entities. If foreign government documents are marked with such a classification designation, whether or not in English, the U.S. classification marking Confidential shall be applied and the Foreign Government Information so designated shall be protected as U.S. Confidential information.

(c) Dates for declassification or for review for declassification shall be marked on foreign government documents only as required by §§ 17.88 and 17.89.

(d) In most cases, other marking requirements prescribed by this regulation for U.S. classified documents are not applicable to documents of foreign governments or international organizations of governments.

§ 17.93 Marking of Foreign Government Information in Department documents.

(a) When Department documents contain Foreign Government Information, the marking “FOREIGN GOVERNMENT INFORMATION” or a marking that otherwise indicates that the information is Foreign Government Information shall be shown on the face of the document.

(b) Where such markings would reveal Foreign Government Information incorporated into Department documents that must be concealed as to its source, the markings shall not be used.

(c) The requirement for portion markings may be satisfied by including the appropriate identification in the portion or paragraph classification markings, e.g., (NATO-S) or (U.K.-C).

§ 17.94 Other Foreign Government Information.

Classified Foreign Government Information held by an Office, Board, Division or Bureau shall be safeguarded or protected as prescribed by this regulation for United States classified information of a comparable level.

Subpart G—Access, Dissemination, and Accountability

§ 17.95 Policy.

(a) No person may be given access to classified information or material originated by, in the custody or under the control of the Department, unless

that person has been determined to be trustworthy and (except as provided in § 17.96(e)) unless access is necessary for the performance of official duties. Procedures shall be established by the Security Program Managers of the Offices, Boards, Divisions and Bureaus to prevent any unnecessary access to classified information. No person is authorized to have access to classified information solely by virtue of rank or position. Accordingly, all requests from the heads of the Offices, Boards, Divisions and Bureaus to the Department Security Officer for a personnel security clearance shall contain a demonstrable need for access to classified information. Further, the number of persons cleared and granted access to classified information shall be maintained at the minimum number that is consistent with operational requirements and needs.

(b) The determination of trustworthiness for eligibility for access to classified information (referred to as a security clearance) shall be made by the Department Security Officer or his designee and shall be based on appropriate security background investigations in accordance with applicable Executive Orders, Department regulations, Intelligence Community directives and Office of Personnel Management guidelines. Current and valid clearances issued to persons by other agencies of the Executive Branch may be accepted, for access purposes only, in lieu of granting such clearances by the Department Security Officer. Such clearance certification shall be accomplished by the Department Security Officer, upon request.

(c) The Department Security Officer may delegate, in writing, the authority to grant Department employees security clearances to qualified Security Programs Managers when the operational need justifies such delegation and the Department Security Officer is assured that such officials shall continually apply all clearance criteria in a uniform and correct manner during the adjudication of personnel security investigations. In those instances where such authority is delegated, the Department Security Officer shall reserve

the right to review all personnel security cases which contain derogatory information that could be a deterrent to eligibility for clearance. The Department Security Officer shall reserve the right to withdraw such authority in any instance where it is determined that Department clearance policy and criteria set forth herein are not being expressly followed.

§ 17.96 Access by persons outside the Executive Branch.

Classified information shall not be disseminated outside the Executive Branch except under conditions that ensure that the information will be given protection equivalent to that afforded within the Executive Branch.

(a) *General.* In accordance with the provisions of Department Order 2620.6, classified information originated by, or in the custody of, the Department may be made available to individuals or agencies outside the Executive Branch provided that such information is necessary for performance of a function from which the Government will derive a benefit or advantage, and that such release is approved by the Attorney General or the Assistant Attorney General for Administration, and is not prohibited by the originating department or agency (or foreign government in the case of Foreign Government Information). Recipients must be shown to be trustworthy by the Department Security Officer and recipients must agree to safeguard the information in accordance with the provisions of this regulation. Heads of Offices, Boards, Divisions and Bureaus shall determine, prior to the release of classified information, the propriety of such action, in the interest of the national security and the recipient's security clearance status and need-to-know.

(b) *Congress.* Access to classified information by Congress, its committees, members, and staff representatives shall be in accordance with the provisions of Department Order 2620.6. Any Department employee testifying before a Congressional Committee in executive session in relation to a classified matter shall obtain the assurance of the committee that individuals present have a security clearance commensurate with the highest classification of

the information that may be discussed. Members of Congress, by virtue of their elected positions, are not investigated or cleared by the Department.

(c) *Non-contractor personnel.* Personnel outside the Executive Branch who are not subject to any Department contracts or grants and therefore are exempt from the provisions of the Defense Industrial Security Program and who require access to classified information originated by or in the custody of the Department shall be processed for such clearance in accordance with the provisions of Department Order 2620.6.

(d) *Contractor personnel.* Personnel who are subject to a Department contract or grant or who are rendering consultant services to the Department and require access to classified information originated by or in the custody of the Department shall be processed for such access/clearance in accordance with the provisions of the Defense Industrial Security Program and Department Order 2600.3A.

(e) *Historical researchers and former Presidential appointees.* (1) The requirement in § 17.95 that access to classified information may be granted only as is necessary for the performance of official duties may be waived for persons who:

(i) Are engaged in historical research projects or

(ii) Have previously occupied policy-making positions to which they were appointed by the President.

(2) All persons receiving access pursuant to this subparagraph must have been determined to be trustworthy by the Department Security Officer as a precondition before receiving access. such determination shall be based on such investigation as the Department Security Officer deems appropriate. Historical researchers and former Presidential appointees shall not have access to Foreign Government Information without the written permission from appropriate authority of the foreign government concerned.

(3) Waivers of the "need-to-know" requirement under this paragraph may be granted by the Department Security Officer provided that the Security Programs Manager of the Office, Board, Division or Bureau with classification